REMARKS

Initially, in the Office Action dated December 23, 2003, the Examiner objects to the drawings as failing to comply with 37 C.F.R. §1.84(p)(5) because they include reference signs not mentioned in the description. Fig. 9 is object to because the reference numeral "914" is used to designate two elements.

Claims 7 and 12 have been objected to as failing to comply with 37 C.F.R. §1.84(p)(4) because of informalities. Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §112, second paragraph. Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §101. Claim 12 is objected to as being a substantial duplicate of claim 7.

Claims 1, 4-7 and 10-12 have been rejected under 35 U.S.C. §102(a) as being anticipated by EP 0 874 307 A1 (Vanstone et al.). Claims 1, 6, 7 and 12 have been rejected under 35 U.S.C. §102(b) as being anticipated by "An Implementation of Elliptic Curve Cryptosystems Over F2155", pages 804-813 (Agnew et al.). Claims 2, 3, 8 and 9 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Vanstone et al. in view of "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests" (Chudnovsky et al.).

By the present response, Applicant has canceled claims 1, 4, 5, 7 and 10-12. Applicant has amended the specification and drawings to further clarify the invention. Further, Applicant has amended claims 2, 3, 6, 8 and 9 to further clarify the invention. Claims 2, 3, 6, 8 and 9 remain pending in the present application.

Drawings Objections

The drawings have been objected to as failing to comply with 37 C.F.R. §1.84(p)(5). Applicant has amended the specification to further clarify the invention and respectfully request that these objections be withdrawn.

The drawings have been objected to as failing to comply with 37 C.F.R. §1.84(p)(4). Applicant has amended the figures to further clarify the invention and respectfully request that these objections be withdrawn.

Claim Objections

Claims 7 and 12 have been objected to because of informalities. Applicant has canceled these claims therefore rendering these rejections moot.

35 U.S.C. §112 Rejections

Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §112, second paragraph. Regarding claims 1, 4, 5, 7 and 10-12, Applicant has canceled these claims therefore rendering these rejections moot. Regarding claims 2, 3, 8 and 9, Applicant has amended the claims to further clarify the invention and respectfully request that these rejections be withdrawn.

35 U.S.C. §101 Rejections

Claims 1-5 and 7-12 have been rejected under 35 U.S.C. §101. Applicant has amended the claims of the present application to further clarify the invention and respectfully request that these rejections be withdrawn.

Double Patenting

Claim 12 has been objected to under 37 C.F.R. §1.75 as being a substantial duplicate of claim 7. Applicant has canceled these claims therefore rendering these objections moot.

35 U.S.C. §102 Rejections

Claims 1, 4-7 and 10-12 have been rejected under 35 U.S.C. §102(a) as being anticipated by Vanstone et al. Applicant has canceled claims 1, 4, 5, 7 and 10-12 therefore rendering these rejections moot. Applicant respectfully traverses these rejections as to remaining pending claim 6.

Vanstone et al. discloses multiplication of a point P on an elliptic curve E by a value K in order to derive a point KP that includes representing the number K as vector of binary digits stored in a register and forming a sequence of point pairs wherein the point pairs differed most by P and wherein the success of series of point pairs are selected by one of two computations. The computations may be performed without using the y-coordinate of the points during the computation while allowing the y-coordinate to be extracted at the end of the computations, thus avoiding the use of inversion operations during the computation and therefore, speeding up the cryptographic processor functions.

Regarding claim 6, Applicant submits that Vanstone et al. does not disclose or suggest the limitations in the combination of this claim of, inter alia, an apparatus implementing an elliptic curve cryptographic operation that includes random number generating means for generating a random number k and projective coordinate

transformation means receiving as inputs thereto coordinate x0 of the finite field of characteristic 2 and the random number k, to thereby transform the coordinate x0 into projective coordinates $[kx0, k] = [x_1, z_1]$. Vanstone et al. does not disclose or suggest these limitations in the claims of the present application. The Examiner fails to issue a proper 102 rejection in that the Examiner fails to specifically point out in the cited reference where each specific limitation is disclosed or suggested in the cited reference. Applicant respectfully asks the Examiner to point out the specific portions in a cited reference that the Examiner asserts discloses or suggests a limitation in the claims of the present application. Here, the Examiner merely references four pages of the Vanstone et al. reference (pages 5-8). These pages of Vanstone et al. merely disclose the multiplication method of Vanstone et al. These portions do not disclose or suggest a random number generating means for generating a random number k or projective coordinate transformation means receiving as inputs thereto coordinate x0 of a finite field of characteristic 2 and a random number k to thereby transform the coordinate x0 into projective coordinates $[kx0, k] = [x_1, z_1]$, as recited in the claims of the present application.

Accordingly, Applicant submits that Vanstone et al. does not disclose or suggest the limitations in the combination of claim 6 of the present application. Applicant respectfully requests that these rejections be withdrawn and that this claim be allowed.

Claims 1, 6, 7 and 12 have been rejected under 35 U.S.C. §102(b) as being anticipated by Agnew et al. Claims 1, 7 and 12 have been canceled therefore

rendering these rejections moot. Applicant respectfully traverses these rejections as to remaining pending claim 6.

Agnew et al. discloses how protocols related to the use of the discreet logarithm problem in public key cryptosystems can be efficiently implemented using the group of an elliptic curve over a finite field. A new VLSI implementation of F_2^{155} and the performance of elliptic curve systems over this ground field is further disclosed.

Regarding claim 6, Applicant submits that Agnew et al. does not disclose or suggest the limitations in the combination of this claim of, inter alia, an apparatus implementing an elliptic curve cryptographic operation that includes random number generating means for generating a random number k and projective coordinate transformation means receiving as inputs thereto coordinate x0 of the finite field of characteristic 2 and the random number k, to thereby transform the coordinate x0 into projective coordinates $[kx0, k] = [x_1, z_1]$. Agnew et al. does not disclose or suggest these limitations in the claims of the present application. Again, the Examiner fails to issue a proper 102 rejection in that the Examiner fails to specifically point out in the cited reference where each specific limitation is disclosed or suggested in the cited reference. Applicant respectfully asks the Examiner to point out the specific portions in a cited reference that the Examiner asserts discloses or suggests a limitation in the claims of the present application. The Examiner again merely references pages (10) of the Agnew et al. reference (pages 804-813). These pages of Agnew et al. are ALL of the pages of Agnew et al. and disclose the elliptic

curve cryptosystems implementation of Agnew et al. These portions do not disclose or suggest a random number generating means for generating a random number k or projective coordinate transformation means receiving as inputs thereto coordinate x0 of a finite field of characteristic 2 and a random number k to thereby transform the coordinate x0 into projective coordinates [kx0, k] = [x_1, z_1], as recited in the claims of the present application. These features according to the present invention, result in randomizing data of coordinate components from applying a generated random number to the respective components.

Accordingly, Applicant submits that Agnew et al. does not disclose or suggest the limitations in the combination of claim 6 of the present application. Applicant respectfully requests that these rejections be withdrawn and that this claim be allowed.

35 U.S.C. §103 Rejections

Claims 2, 3, 8 and 9 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Vanstone et al. in view of Chudnovsky et al. Applicant respectfully traverses these rejections.

Chudnovsky et al. discloses sequences of numbers generated by addition in formal groups and new primality and factorization tests where new methods are presented for primality testing and generating of big prime numbers, and disclosure related to new versions of factorization methods.

Applicant submits that neither Vanstone et al. nor Chudnovsky et al., taken alone or in any proper combination, disclose, suggest or render obvious the

limitations in the combination of each of these claims of, inter alia, generating a random number k, transforming the x-coordinates into projective coordinates to thereby derive projective coordinates [k^x, k] through arithmetic operation of individual coordinate components of the projective space and the stored random number k, or transforming the x-coordinates into projective coordinates to thereby derive projective coordinates [kx, k] through arithmetic operation of individual coordinate components of the projective space and the stored random number k. These limitations are neither disclosed nor suggested by Vanstone et al. nor Chudnovsky et al. The Examiner admits that Vanstone et al. does not disclose or suggest a random number being used to device projective coordinates, but asserts that Chudnovsky et al. discloses methods for improving the speed of elliptic curves and therefore the Examiner believes the teachings of these two references would render the claims of the present application obvious, if the scope of the claims were clearly defined. However, Chudnovsky et al. relates to presenting methods for primality testing and generation of big prime numbers and new versions of factorization methods. Neither Vanstone et al. nor Chudnovsky et al. disclose or suggest generating a random number k, or transforming the x-coordinates into projective coordinates to thereby derive projective coordinates either [kx, k] or [k^2x, k], through arithmetic operation of individual coordinate components of the projective space and the stored random number k, as recited in the claims of the present application. These features according to the present invention, result in randomizing

data of coordinate components from applying a generated random number to the respective components.

Accordingly, Applicant submits that neither Vanstone et al. nor Chudnovsky et al. taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 2, 3, 8 and 9 of the present application. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicant submits that claims 2, 3, 6, 8 and 9 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicant petitions for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 500.38035X00).

Respectfully submitted,

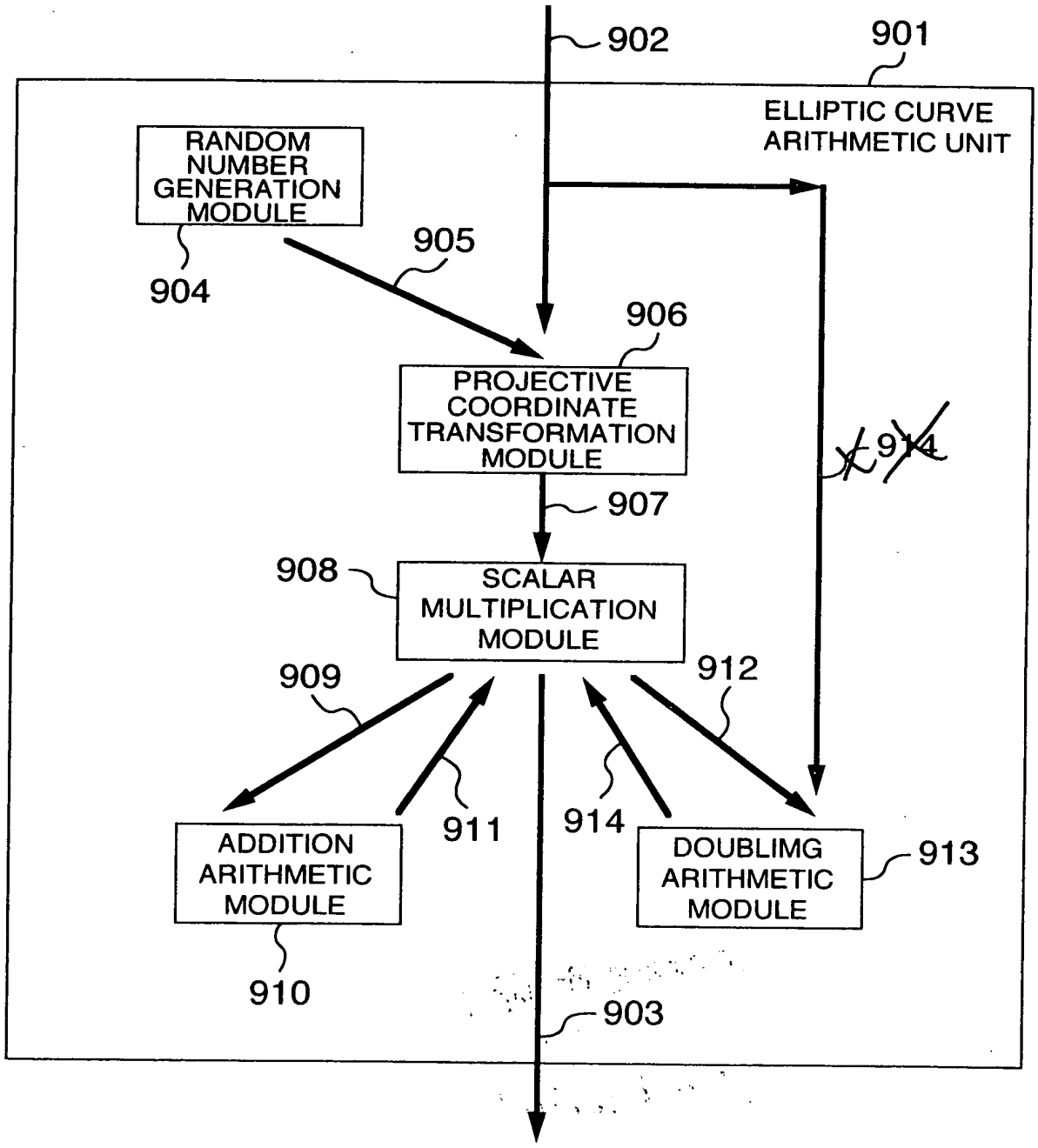
ANTONELLI, TERRY, STOUT & KRAUS, LLP

Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600

Attachment: Replacement Sheet
Annotated Sheet Showing Changes

FIG. 9



approved DTM 25 May 2004